DEFENSE INFORMATION SYSTEMS AGENCY
JOINT INTEROPERABILITY TEST COMMAND
P.O. BOX 12798
FORT HUACHUCA, ARIZONA 85670-2798

IN REPLY REFER TO: Networks and Transport Division (JTE) 4 October 2006

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of Cisco Assured Services Voice Application Local Area Network (ASVALAN) with Specified Software Releases

References: (a) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01D, "Interoperability and Supportability of Information Technology and National Security Systems," 8 March 2006

1. References (a) and (b) establish the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification. Additional references are provided in enclosure 1.

2. The Cisco ASVALAN with specified software releases is hereinafter referred to as the system under test (SUT). The SUT meets all of its critical interoperability requirements and is certified as interoperable for joint use within the Defense Switched Network (DSN). The SUT is certified to support DSN assured services over Internet Protocol. The SUT components, which are bolded and underlined in the tables throughout this certification letter, are components that were tested in the JITC laboratory for this certification. The SUT components, which are not bolded and not underlined, but also listed throughout the tables in this letter, are certified for joint use in the DSN as well. However, these components are certified via JITC analysis. The JITC analysis determined these components to contain same hardware and software and to be functionally identical to the tested components for interoperability certification purposes. Testing did not include video services or data applications; however, simulated data traffic was generated during testing to determine its effect on voice traffic. This certification expires upon changes that could affect interoperability, but no later than three years from the date of this memorandum.

3. This finding is based on interoperability testing conducted by JITC and a review of the vendor's Letters of Compliance (LoC). Testing was conducted at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona, from 1 through 26 May 2006. Review of the vendor's LoC was completed on 11 August 2006. Enclosure 2 documents the test results and describes the tested network. System interoperability should be verified before deployment in an operational environment that varies significantly from the test environment.

4. The overall interoperability status of the SUT is indicated in table 1. The ASVALAN system requirements are listed in table 2. In addition to system level requirements, components that comprise the SUT must meet specific criteria to be certified for use as core, distribution, or access components. The interoperability status of the SUT components is listed in table 3. The

requirements used to certify the components are listed in table 4. This interoperability test status is based on the SUT's ability to meet:

a. Local Area Network system requirements specified in reference (c) verified through JITC testing and/or vendor submission of LoC.

b. Internet Protocol version 6 requirements specified in reference (c), paragraph 1.7, table 1-3, by 30 June 2008 in accordance with reference (d) verified through vendor submission of LoC signed by the Vice President of the company.

c. Assured services as defined in reference (e).

d. The overall system interoperability performance derived from test procedures listed in reference (f).

Table 1. SUT Interoperability Status

System Interoperability Status			
Components[1]	**Release**	**Status**	**Remarks**
Cisco **6509**/6509-NEB/6509-NEB-A/ 6503/6506/6513 Catalyst Switches	Native IOS 12.2 (18) SXF3	Certified	All ASVALAN system requirements were met when the SUT was configured in accordance with architecture provided in enclosure 2.[3] Additional details about component level certification are provided in table 3.
Cisco **4507R**/4503[2]/4506[2] /4510R Catalyst Switches	IOS 12.2 (31) SG		
Catalyst 3750[2] (WS-C3750G-12S-E)	12.2 (25) SEE		
Catalyst 3560 – PoE 24 / Catalyst 3560	12.2 (25) SEE2		
Catalyst 2960 – Inline Power	12.2 (25) SEE		
ONS 15454	7.0		
Catalyst 2940	12.1 (22) EA7	Certified	See note 4.
Catalyst 2950	12.1 (22) EA7		
Catalyst 2960	12.2 (25) SEE Release Software (fc2)		

LEGEND:

ASVALAN	- Assured Services Voice Application LAN	JITC	- Joint Interoperability Test Command
DISA	- Defense Information Systems Agency	LAN	- Local Area Network
DSN	- Defense Switched Network	NEB	- Network Equipment Building
G	- Gigabit	ONS	- Optical Network System
GSCR	- Generic Switching Center Requirements	PoE	- Power over Ethernet
IOS	- Internetworking Operating System	SUT	- System Under Test
IPv6	- Internet Protocol version 6	WS	- Workgroup Station

NOTES:

1 Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same IOS software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.

2 Indicates these switches support one processor and must be configured to fail over to a redundant distribution switch.

3 LAN security testing is accomplished through DISA-led Information Assurance testing and evaluation. Results are published in a separate report.

4 All of the SUT components covered under this certification met the IPv6 criteria with the exception of the Catalyst 2940 and the Catalyst 2950. The Catalyst 2940 and the Catalyst 2950 do not meet the critical IPv6 capability requirement in accordance with the GSCR, paragraph 1.7. However, components that are not currently IPv6 capable and have been identified by the vendor as having no migration path to IPv6, may be certified if the following criteria are met:
   a. The component must already be JITC certified and currently fielded within the DSN.
   b. There must be a certified, IPv6-capable component available for replacement. To meet this requirement Cisco has designated the Catalyst 2960 as a replacement.

Table 2. ASVALAN System Requirements

System Requirements			
Requirement	**Criteria**	**Reference**	**Critical**
Delay	One-way packet delay for voice packets of an established call (signaling and media) shall be 5 ms or less averaged over any 5-minute period.	GSCR, Appendix 3, Section A.3.3.1.1	Yes
Jitter	For voice media packets, jitter shall be 5 ms or less averaged over any 5-minute period.	GSCR, Appendix 3, Section A.3.3.1.2	Yes
Packet Loss	Voice packet loss within the LAN shall not exceed 0.05% averaged over any 5-minute period.	GSCR, Appendix 3, Section A.3.3.1.3	Yes
Reliability	- LANs shall have a reliability of .99999 - No single point of failure for outage of more than 64 telephony subscribers - Maximum downtime of 35 mins/yr for network links and 12 mins/yr for IP subscribers - Network Path restores within 2 seconds	GSCR, Appendix 3, Section A.3.3.4.1	Yes
IPv6[1]	All IP devices shall be IPv6 capable.	GSCR, Appendix 3, Section A3.2.8, Paragraph 1.7	Yes
Security[2]	DITSCAP/IA	GSCR, Appendix 3, Section A.3.3.4.3	Yes

LEGEND:

ASVALAN	- Assured Services Voice Application LAN	IPv4	- Internet Protocol version 4
DISA	- Defense Information Systems Agency	IPv6	- Internet Protocol version 6
DITSCAP	- DoD IT Security Certification and Accreditation Process	IT	- Information Technology
DoD	- Department of Defense	LAN	- Local Area Network
GSCR	- Generic Switching Center Requirements	mins	- minutes
IA	- Information Assurance	ms	- milliseconds
IP	- Internet Protocol	yr	- year

NOTES:

1 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of their respective company. The vendor must state, in writing, compliance to the following criteria by 30 June 2008**:**

a. Conformant with IPv6 standards profile contained in the DoD IT Standards Registry (DISR).
b. Maintaining interoperability in heterogeneous environments and with IPv4.
c. Commitment to upgrade as the IPv6 standard evolves.
d. Availability of contractor/vendor IPv6 technical support.

2 Information assurance testing is accomplished via DISA-led Information Assurance test teams and published in a separate report.

Table 3. SUT Component Interoperability Status

Component Interoperability Status				
Component[1]	**Release**	**Sub-component[1]**	**Status**	**Remarks**
Cisco **6509**/6509-NEB/6509-NEB-A/ 6503/6506/6513 Catalyst Switches	Native IOS 12.2 (18) SXF3 Release Software (fc1)	**WS-SUP720-3B**[3]	Certified	All Core, Distribution, and Access requirements were met.
		WS-SUP720-3BXL[3]	Certified	
		WS-SUP720[3]	Certified	
		WS-X6816-GBIC	Certified	
		WS-X6748-SFP	Certified	
		WS-X6724-SFP	Certified	
		WS-X6148-RJ45V	Certified	
		WS-X6148-45AF	Certified	
		WS-X6148A-GE-45AF	Certified	
		WS-X6748-GE-TX	Certified	
		WS-X6704-10GE	Certified	
		WS-X6548-GE-45AF	Certified	
		WS-X6548V-GE-TX	Certified	
		WS-X6548-GE-TX	Certified	
		WS-X6548-RJ-21	Certified	
		WS-X6548-RJ-45	Certified	
		WS-X6516-GBIC	Certified	
		WS-X6516A-GBIC	Certified	
		WS-X6516-GE-TX	Certified	
		WS-X6148V-GE-TX	Certified	
		WS-X6148-RJ-45	Certified	
		WS-X6148-RJ-21	Certified	
		WS-X6148-RJ21V	Certified	
		WS-X6148-21AF	Certified	
		WS-X6148-GE-TX	Certified	
		WS-X6148-GE-45AF	Certified	
		WS-X6148A-GE-TX	Certified	
		WS-X6148A-45AF	Certified	
Cisco **4507R**/4503[2] /4506[2]/4510R Catalyst Switches	IOS 12.2 (31) SG Release Software (fc2)	**WS-X4515 Sup Engine IV**[3]	Certified	All Core, Distribution, and Access requirements were met.
		WS-X4516-10GE Sup Engine V[3]	Certified	
		WS-X4516 (Sup V)		
		WS-X4306-GB	Certified	
		WS-X4302-GB	Certified	
		WS-X4148-RJ45V	Certified	
		WS-X4148-RJ45	Certified	
		WS-X4124-RJ45	Certified	
		WS-X4148-RJ21	Certified	
		WS-X4248-RJ45V	Certified	
		WS-X4248-RJ21V	Certified	
		WS-X4548-GB-RJ45V	Certified	
		WS-X4524-GB-RJ45V	Certified	
		WS-X4548-GB-RJ45	Certified	
Catalyst 3750[2] (WS-C3750G-12S-E)	12.2 (25) SEE Release Software (fc2)		Certified	All Distribution requirements were met.
Catalyst 3560 – PoE 24 / Catalyst 3560	12.2 (25) SEE2 Release Software (fc2)		Certified	All Access requirements were met.

Table 3. SUT Component Interoperability Status (continued)

Component Interoperability Status				
Component[1]	**Release**	**Sub-component[1]**	**Status**	**Remarks**
Catalyst 2940	12.2 (22) EA7		Certified	See note 4.
Catalyst 2950	12.2 (22) EA7		Certified	See note 4.
Catalyst 2960	12.2 (25) SEE Release Software (fc2)		Certified	All Access requirements were met.
ONS 15454	Release 7.0	**15454-ML1000-2-NTE**	Certified	All network element requirements were met.
		15454-ML100T-12	Certified	
		15454-TCC2P	Certified	
		15454-XC-VXC-10G	Certified	
		15454-XC-10G-S1	Certified	
		15454-MRC-I-12	Certified	

LEGEND:

802.3af	- Standard for Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI)	MRC	- Multirate Optic Card
		NEB	- Network Equipment Building
		NTE	- Network Services Engine
AF	- PoE IEEE 802.3af Standard	ONS	- Optical Network System
B/BXL	- Version B, eXtra Large Memory	PoE	- Power Over Ethernet
DSN	- Defense Switched Network	RJ	- Registered Jack
E	- Ethernet	SFP	- Small Form Factor Pluggable
G, GB	- Gigabit	SUP	- Supervisor
GBIC	- Gigabit Interface Card	SUT	- System Under Test
GE	- Gigabit Ethernet	TCC2P	- Timing, Communications and Control -version 2 Plus
GSCR	- Generic Switching Center Requirements	TX	- Twisted Pair
IEEE	- Institute of Electrical and Electronics Engineers, Inc.	V	- Voice
IOS	- Internetworking Operating System	VXC	- Very Large Cross Connect
IPv6	- Internet Protocol version 6	WS	- Workgroup Station
JITC	- Joint Interoperability Test Command	XC	- Cross Connect
ML	- Multilayer		

NOTES:

1 Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same IOS software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.

2 Indicates these switches support one processor and must be configured to fail over to a second distribution switch.

3 The Supervisor Engines were tested and certified with the exception of the GE and 10 GE uplink ports. These ports were not tested and are not certified.

4 All of the SUT components covered under this certification met the IPv6 criteria with the exception of the Catalyst 2940 and the Catalyst 2950. The Catalyst 2940 and the Catalyst 2950 do not meet the critical IPv6 capability requirement in accordance with the GSCR, paragraph 1.7. However, components that are not currently IPv6 capable and have been identified by the vendor as having no migration path to IPv6, may be certified if the following criteria are met:

a. The component must already be JITC certified and currently fielded within the DSN.

b. There must be a certified, IPv6-capable component available for replacement. To meet this requirement Cisco has designated the Catalyst 2960 as a replacement.

Table 4. ASVALAN Component Requirements

Core/Distribution/Access Component Requirements			
Requirement	**Criteria**	**Reference**	**Critical**
CoS Models	LAN components shall support IEEE 802.1p to DSCP mapping and at least one of the following: - IEEE 802.1p/Q priority tagging/VLAN tagging - DSCP - ToS	GSCR, Appendix 3, Section A.3.3.2.1	Yes
Traffic Prioritization	Traffic within LAN components shall be prioritized so that voice signaling receives highest priority, voice media second highest priority, and data lowest priority.	GSCR, Appendix 3, Section A.3.3.2.2	Yes
QoS	LAN components shall support one of the following: - Priority Queuing - Custom Queuing - Weighted Fair Queuing - Class Based Weighted Fair Queuing	GSCR, Appendix 3, Section A.3.3.3.1	Yes

Table 4. Component Requirements (continued)

Core/Distribution/Access Component Requirements			
Requirement	**Criteria**	**Reference**	**Critical**
Policing	LAN components shall support one of the following: - DSCP PHB - Generic Traffic Shaping - Class-Based Shaping	GSCR, Appendix 3, Section A.3.3.3.2	Yes
VLANs	LAN components shall support: - Port based VLANs - MAC address based VLANs - Protocol based VLANs	GSCR, Appendix 3, Section A.3.3.3.3	Yes
IEEE Conformance	LAN components shall support: - IEEE 802.1d – Bridging - IEEE 802.1 p/Q – Priority tagging/VLAN tagging - IEEE 802.1s – Per-VLAN Group Spanning Tree - IEEE 802.1v – VLAN Classification by port and protocol - IEEE 802.1w –Rapid Reconfiguration of Spanning Tree - IEEE 802.1x – Port Based Network Access Control - IEEE 802.3ad – Link Aggregation Protocol	GSCR, Appendix 3, Section A.3.3.4	Yes
Reliability	LAN components shall support: - Dual power supplies and Dual processors (more than 64 users) - N+1 sparing for access (more than 64 users) - Redundancy protocol[1] - 2 second path restoral	GSCR, Appendix 3, Section A.3.3.4.1	Yes
Network Management	LAN components shall support: - In-band or out-of-band management - SNMP - Measurements	GSCR, Appendix 3, Section A.3.3.4.2	Yes
Security	LAN components shall employ the Network Infrastructure and VoIP STIGs.[2]	GSCR, Appendix 3, Section A.3.3.4.3	Yes
IPv6	All IP devices shall be IPv6 capable.[3]	GSCR, Appendix 3, Section A3.2.8, Paragraph 1.7	Yes
TE	- LAN components shall be engineered for a maximum of 25% voice traffic per link.[4] - For more than 64 users, link pairs (redundant links) must be used.	GSCR, Appendix 3, Section A.3.3.4.4	Yes

LEGEND:

ASVALAN	- Assured Services Voice Application LAN	Mbps	- Megabits per second
CoS	- Class of Service	N	- total VoIP users / 64
DISA	- Defense Information Systems Agency	PHB	- Per Hop Behaviors
DSCP	- Differentiated Services Code Point	QoS	- Quality of Service
GSCR	- Generic Switching Center Requirements	SNMP	- Simple Network Management Protocol
IEEE	- Institute of Electrical and Electronics Engineers, Inc	STIGs	- Security Technical Implementation Guides
IP	- Internet Protocol	TE	- Traffic Engineering
IPv4	- Internet Protocol version 4	ToS	- Type of Service
IPv6	- Internet Protocol version 6	VLANs	- Virtual LANs
LAN	- Local Area Network	VoIP	- Voice over Internet Protocol
MAC	- Media Access Control	VRRP	- Virtual Router Redundancy Protocol

NOTES:

1 For core and distribution components, redundancy protocol shall be the routing protocol supported. For access components, redundancy protocol shall be VRRP or equivalent protocol.

2 Verified using the Information Assurance Test Plan. Results of the security testing are published in a separate test report generated by the DISA Information Assurance test personnel.

3 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of their respective company. The vendor must state, in writing, compliance to the following criteria by 30 June 2008**:**

a. Conformant with IPv6 standards profile contained in the Department of Defense Information Technology Standards Registry (DISR).
b. Maintaining interoperability in heterogeneous environments and with IPv4.
c. Commitment to upgrade as the IPv6 standard evolves.
d. Availability of contractor/vendor IPv6 technical support.

4 Instruments connected to an access device must provide a minimum of a 10 Mbps full duplex link. For core and distribution connections, the minimum link capacity is 100 Mbps full duplex.

5. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and

references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil (NIPRNet), or http://199.208.204.125 (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.

6. The JITC point of contact is Mr. Joseph Schulte, DSN 879-5164, commercial (520) 538-5164, FAX DSN 879-4347, or e-mail to joseph.schulte@disa.mil. The tracking number for the SUT is 0531201.

FOR THE COMMANDER:

2 Enclosures a/s

RICHARD A. MEADOR
Chief
Networks and Transport Division

Distribution:
Joint Staff J6I, Room 1E596, Pentagon, Washington, DC 20318-6000
Joint Interoperability Test Command, Liaison, ATTN: TED/JT1, 2W24-8C, P.O. Box 4502, Falls Church, VA 22204-4502
Defense Information Systems Agency, Net-Centricity Requirements and Assessment Branch, ATTN: GE333, Room 244, P.O. Box 4502, Falls Church, VA 22204-4502
Office of Chief of Naval Operations (N71CC2), CNO N6/N7, 2000 Navy Pentagon, Washington, DC 20350
Headquarters U.S. Air Force, AF/XICF, 1800 Pentagon, Washington, DC 20330-1800
Department of the Army, Office of the Secretary of the Army, CIO/G6, ATTN: SAIS-IOQ, 107 Army Pentagon, Washington, DC 20310-0107
U.S. Marine Corps (C4ISR), MARCORSYSCOM, 2200 Lester St., Quantico, VA 22134-5010
DOT&E, Net-Centric Systems and Naval Warfare, 1700 Defense Pentagon, Washington, DC 20301-1700
U.S. Coast Guard, CG-64, 2100 2nd St. SW, Washington, DC 20593
Defense Intelligence Agency, 2000 MacDill Blvd., Bldg 6000, Bolling AFB, Washington, DC 20340-3342
National Security Agency, ATTN: DT, Suite 6496, 9800 Savage Road, Fort Meade, MD 20755-6496
Director, Defense Information Systems Agency, ATTN: GS235, Room 5W24-8A, P.O. Box 4502, Falls Church, VA 22204-4502
Office of Assistant Secretary of Defense (NII)/DoD CIO, Crystal Mall 3, 7th Floor, Suite 7000, 1851 S. Bell St., Arlington, VA 22202
Office of Under Secretary of Defense, AT&L, Room 3E144, 3070 Defense Pentagon, Washington, DC 20301
U.S. Joint Forces Command, J68, Net-Centric Integration, Communications, and Capabilities Division, 1562 Mitscher Ave., Norfolk, VA 23551-2488
Defense Information Systems Agency (DISA), ATTN: GS23 (Mr. Osman), Room 5w23, 5275 Leesburg Pike (RTE 7), Falls Church, VA 22041

ADDITIONAL REFERENCES

(c) Defense Information Systems Agency (DISA), "Defense Switched Network (DSN) Generic Switching Center Requirements (GSCR), Appendix 3, (Incorporated Change 1)," 1 March 2005
(d) Executive Office of the President, "Transition Planning for Internet Protocol version 6 (IPv6)," 2 August 2005
(e) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01B, "Policy for Department of Defense Voice Services," 23 September 2001
(f) Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP), Change 1, Revision 1," 1 June 2005

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Cisco Assured Services Voice Application Local Area Network (ASVALAN) with specified software releases, hereinafter referred to as the system under test (SUT).

2. PROPONENT. Defense Information Systems Agency (DISA).

3. PROGRAM MANAGER. Mr. Howard Osman, GS23, Room 5W23, 5275 Leesburg Pike, Falls Church, VA 22041, E-mail: Howard.Osman@disa.mil.

4. TESTER. Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.

5. SYSTEM UNDER TEST DESCRIPTION. The SUT is an ASVALAN. An ASVALAN is used to transport voice signaling and media as part of an overall Voice over Internet Protocol (VoIP) system. The SUT consisted of the following devices:

a. Core: The Catalyst 6500 series switches can be used as core, distribution, or access switches. The Catalyst 6509 switch with Native Internetworking Operating System (IOS) 12.2 (18) SXF3, delivers scalable performance and port density across several chassis configurations. The Catalyst 6500 series is available in 3-, 6-, 9-, and 13-slot chassis. The Catalyst 6500 series switches feature a range of integrated services modules, including 10-gigabit fiber cards, gigabit fiber cards, and 10/100/1000 Megabits per second (Mbps) switchblades used as access points. For data and voice applications, users can connect to the Local Area Network (LAN) using the 10/100/1000 Base-T Ethernet interface on the access devices.

The Cisco Catalyst 4500 series switches with IOS 12.2 (31) SG can be used as core, distribution, or access switches. The 4500 series is available in a multi-slot chassis for gigabit fiber cards and 10/100/1000 Mbps access points to the LAN. This framework allows flexibility in creating a switching platform and also allows for a highly redundant architecture to ensure no single point of failure for hardware operations. Some slots are reserved for special functions such as supervisor engines. Most slots are flexible and can be configured for specific user needs. One benefit of this system is the ability to add, delete, and change system elements over time. All line card capabilities including bandwidth, throughputs, and routing are dependent on the supervisor engine.

b. Distribution: The Cisco Catalyst 3750 series (WS-C3750G-12S-E) with IOS 12.2 (25) SEE can be used in the distribution layer only. The 3750 distribution switch consists of 12 1-gigabit Ethernet fiber ports. The Catalyst 3750 contains a single processor and power supply and therefore must be configured to fail over to a redundant distribution switch. In the current configuration, the 4507R with IOS 12.2 (31) SG served as the redundant distribution switch.

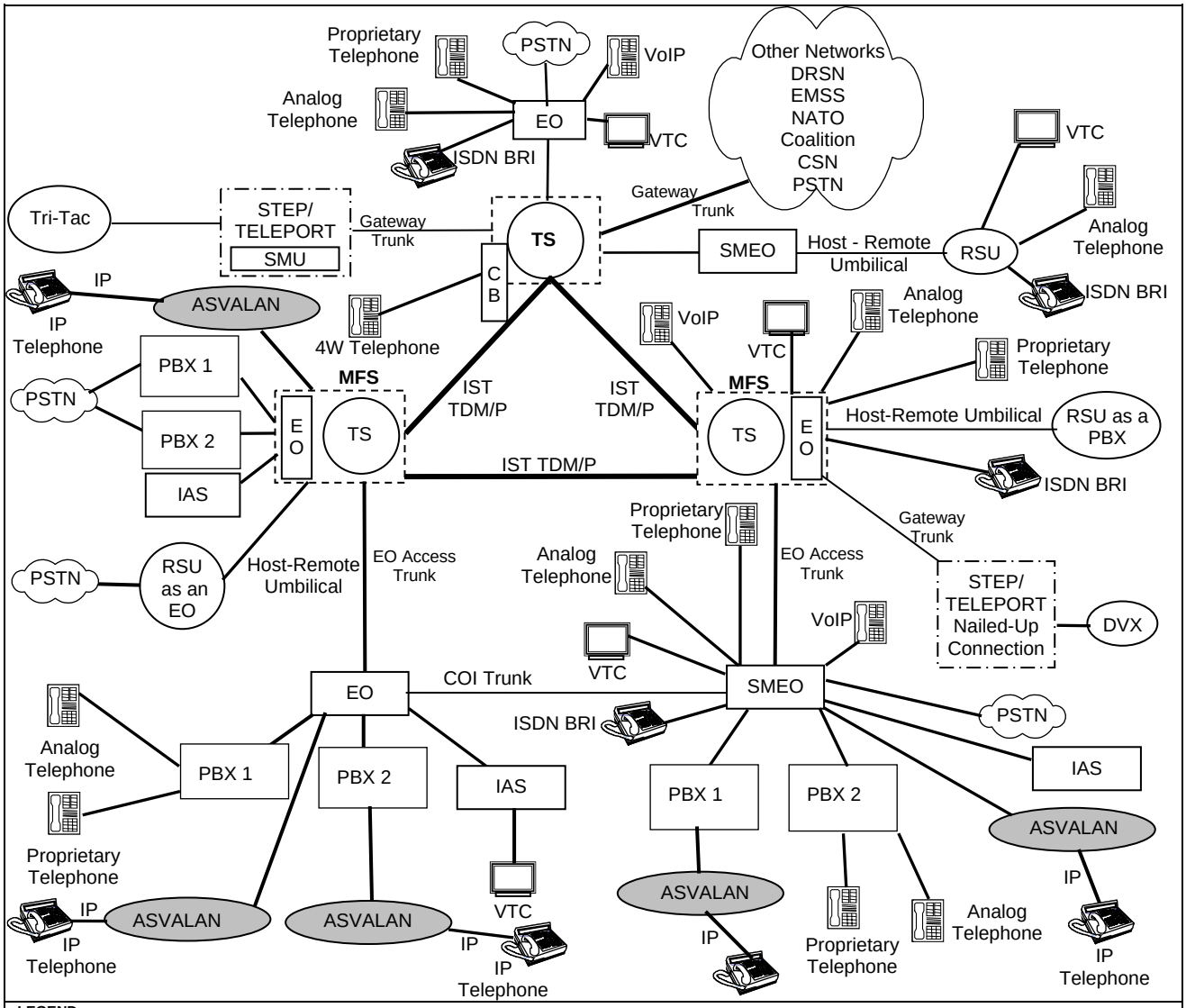
c. Access: The Cisco Catalyst 3560 and the Catalyst 2960 with release 12.2 (25) SEE2, the Catalyst 2950, and the Catalyst 2940 with release 12.1 (22) EA7 can be used

in the access layer only. The 3560 Catalyst switch provides Power over Ethernet (PoE) to any device that complies with the Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.3af standard. All of the access switches provide high availability, security and Quality of Service (QoS) to meet the operation requirements of the network. Security access control lists can be implemented, as well as QoS, rate-limiting, multicast management, and IP routing. The Catalyst 3560 has 24 10/100 Mbps copper ports and two 1-gigabit uplink ports and is a layer 3 (L3) switch. The Catalyst 2960 and 2950 have 48 10/100 Mbps copper ports and two 1-gigabit uplink ports and are layer 2 (L2) switches. The Catalyst 2940 has eight 10/100 Mbps copper ports and one 1-gigabit uplink port and a 100 Mbps fiber uplink port and is an L2 switch.

d. Shared access: Shared access [i.e., same switch port is shared by Personal Computer and Internet Protocol (IP) phone], was tested and is certified with this configuration. The IP phones were connected to the 100 Mbps full duplex access switch port and data was connected to the 100 Mbps Ethernet port on the back of the phones. All switches that provide Ethernet access ports in this certification were tested for shared access with no measurable degradation of voice quality.

e. Network Element: The Cisco Optical Network System (ONS) 15454 combines functions of multiple network elements in a single platform including Synchronous Optical Network (SONET)/Synchronous Digital Hierarchy (SDH) transport, integrated optical networking as well as International Telecommunication Union Grid Wavelengths and Dense Wave Division Multiplexing (DWDM), multiservice interfaces on demand with Ethernet, Asynchronous Transfer Mode (ATM), and Time Division Multiplexing (TDM). ATM and DWDM were not tested and are not covered under this certification. The ONS combines optical transport with IP to deliver the next generation voice and data services. The Cisco ONS 15454 SONET provides TDM solutions with interfaces such as Digital Signal level 1 (DS-1), DS-3, and data solutions with 10/100/1000 Ethernet solutions with Optical Carrier level 3 (OC-3) to OC-192 transport bit rates plus DWDM wavelengths. This certification only covers the ONS as an IP optical transport. TDM interfaces are covered under a separate certification as a Network Element.

6. OPERATIONAL ARCHITECTURE. The Defense Switched Network (DSN) architecture is a two-level network hierarchy consisting of DSN backbone switches and Service/Agency installation switches. Service/Agency installation switches have been authorized to extend voice services over IP infrastructures. The Generic Switching Center Requirements (GSCR) operational DSN Architecture is depicted in figure 2-1. The installation VoIP architecture is depicted in figure 2-2. The VoIP architecture depicts the relationship of DSN ASVALANs to the DSN switch types.



LEGEND:

4W	- 4-Wire
ASVALAN	- Assured Services Voice Application Local Area Network
BRI	- Basic Rate Interface
CB	- Channel Bank
COI	- Community of Interest
CSN	- Canadian Switch Network
DRSN	- Defense Red Switch Network
DSN	- Defense Switched Network
DVX	- Deployable Voice Exchange
EMSS	- Enhanced Mobile Satellite System
EO	- End Office
IAS	- Integrated Access Switch
IP	- Internet Protocol
ISDN	- Integrated Services Digital Network
IST	- Interswitch Trunk
MFS	- Multifunction Switch
NATO	- North Atlantic Treaty Organization
PBX	- Private Branch Exchange
PBX 1	- Private Branch Exchange 1
PBX 2	- Private Branch Exchange 2
PSTN	- Public Switched Telephone Network
RSU	- Remote Switching Unit
SMEO	- Small End Office
SMU	- Switched Multiplex Unit
STEP	- Standardized Tactical Entry Point
TDM/P	- Time Division Multiplex/Packetized
Tri-Tac	- Tri-Service Tactical Communications Program
TS	- Tandem Switch
VoIP	- Voice over Internet Protocol
VTC	- Video Teleconferencing

Figure 2-1. DSN Architecture

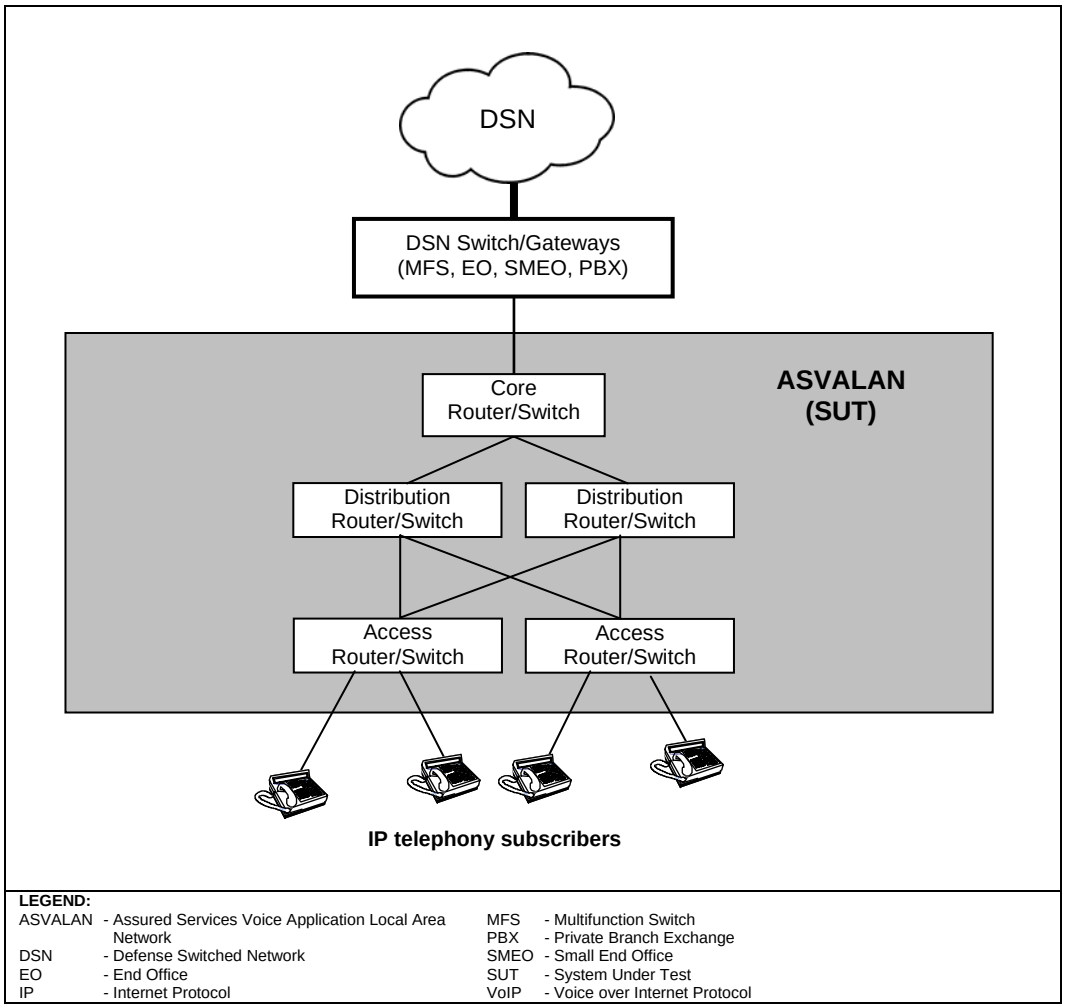


Figure 2-2. VoIP Architecture

7. REQUIRED SYSTEM INTERFACES. Requirements specific to the SUT and its components are listed in table 2-1. The requirements specific to the SUT components are shown in table 2-2. These requirements are derived from:

a. DSN services for Network and Applications specified in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01B, "Policy for Department of Defense Voice Services."

b. GSCR, appendix 3, Capability Requirements (CRs) and Feature Requirements (FRs) verified through JITC testing and/or vendor submission of Letters of Compliance (LoC).

Table 2-1. ASVALAN System Requirements

System Requirements			
Requirement	**Criteria**	**Reference**	**Critical**
Delay	One-way packet delay for voice packets of an established call (signaling and media) shall be 5 ms or less averaged over any 5-minute period.	GSCR, Appendix 3, Section A.3.3.1.1	Yes
Jitter	For voice media packets, jitter shall be 5 ms or less averaged over any 5-minute period.	GSCR, Appendix 3, Section A.3.3.1.2	Yes
Packet Loss	Voice packet loss within the LAN shall not exceed 0.05% averaged over any 5-minute period.	GSCR, Appendix 3, Section A.3.3.1.3	Yes
Reliability	- LANs shall have a reliability of .99999 - No single point of failure for outage of more than 64 telephony subscribers - Maximum downtime of 35 mins/yr for network links and 12 mins/yr for IP subscribers - Network Path restores within 2 seconds	GSCR, Appendix 3, Section A.3.3.4.1	Yes
IPv6[1]	All IP devices shall be IPv6 capable.	GSCR, Appendix 3, Section A3.2.8, Paragraph 1.7	Yes
Security[2]	DITSCAP/IA	GSCR, Appendix 3, Section A.3.3.4.3	Yes

LEGEND:

ASVALAN	- Assured Services Voice Application LAN	IPv4	- Internet Protocol version 4
DISA	- Defense Information Systems Agency	IPv6	- Internet Protocol version 6
DITSCAP	- DoD IT Security Certification and Accreditation Process	IT	- Information Technology
DoD	- Department of Defense	LAN	- Local Area Network
GSCR	- Generic Switching Center Requirements	mins	- minutes
IA	- Information Assurance	ms	- milliseconds
IP	- Internet Protocol	yr	- year

NOTES:

1 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of their respective company. The vendor must state, in writing, compliance to the following criteria by 30 June 2008**:**
   a. Conformant with IPv6 standards profile contained in the DoD IT Standards Registry (DISR).
   b. Maintaining interoperability in heterogeneous environments and with IPv4.
   c. Commitment to upgrade as the IPv6 standard evolves.
   d. Availability of contractor/vendor IPv6 technical support.

2 Information assurance testing is accomplished via DISA-led Information Assurance test teams and published in a separate report.

Table 2-2. ASVALAN Component Requirements

Core/Distribution/Access Component Requirements			
Requirement	**Criteria**	**Reference**	**Critical**
CoS Models	LAN components shall support IEEE 802.1p to DSCP mapping and at least one of the following: - IEEE 802.1p/Q priority tagging/VLAN tagging - DSCP - ToS	GSCR, Appendix 3, Section A.3.3.2.1	Yes
Traffic Prioritization	Traffic within LAN components shall be prioritized so that voice signaling receives highest priority, voice media second highest priority, and data lowest priority.	GSCR, Appendix 3, Section A.3.3.2.2	Yes
QoS	LAN components shall support one of the following: - Priority Queuing - Custom Queuing - Weighted Fair Queuing - Class Based Weighted Fair Queuing	GSCR, Appendix 3, Section A.3.3.3.1	Yes
Policing	LAN components shall support one of the following: - DSCP PHB - Generic Traffic Shaping - Class-Based Shaping	GSCR, Appendix 3, Section A.3.3.3.2	Yes
VLANs	LAN components shall support: - Port based VLANs - MAC address based VLANs - Protocol based VLANs	GSCR, Appendix 3, Section A.3.3.3.3	Yes

Table 2-2. ASVALAN Component Requirements (continued)

Core/Distribution/Access Component Requirements			
Requirement	**Criteria**	**Reference**	**Critical**
IEEE Conformance	LAN components shall support: - IEEE 802.1d – Bridging - IEEE 802.1 p/Q – priority tagging/VLAN tagging - IEEE 802.1s – Per-VLAN Group Spanning Tree - IEEE 802.1v – VLAN Classification by port and protocol - IEEE 802.1w –Rapid Reconfiguration of Spanning Tree - IEEE 802.1x – Port Based Network Access Control - IEEE 802.3ad – Link Aggregation Protocol	GSCR, Appendix 3, Section A.3.3.4	Yes
Reliability	LAN components shall support: - Dual power supplies and Dual processors (more than 64 users) - N+1 sparing for access (more than 64 users) - Redundancy protocol[1] - 2 second path restoral	GSCR, Appendix 3, Section A.3.3.4.1	Yes
Network Management	LAN components shall support: - In-band or out-of-band management - SNMP - Measurements	GSCR, Appendix 3, Section A.3.3.4.2	Yes
Security	LAN components shall employ the Network Infrastructure and VoIP STIGs.[2]	GSCR, Appendix 3, Section A.3.3.4.3	Yes
IPv6	All IP devices shall be IPv6 capable.[3]	GSCR, Appendix 3, Section A3.2.8, Paragraph 1.7	Yes
TE	- LAN components shall be engineered for a maximum of 25% voice traffic per link.[4] - For more than 64 users, link pairs (redundant links) must be used.	GSCR, Appendix 3, Section A.3.3.4.4	Yes

LEGEND:

ASVALAN	- Assured Services Voice Application LAN	Mbps	- Megabits per second
CoS	- Class of Service	N	- total VoIP users / 64
DISA	- Defense Information Systems Agency	PHB	- Per Hop Behaviors
DSCP	- Differentiated Services Code Point	QoS	- Quality of Service
GSCR	- Generic Switching Center Requirements	SNMP	- Simple Network Management Protocol
IEEE	- Institute of Electrical and Electronics Engineers, Inc	STIGs	- Security Technical Implementation Guides
IP	- Internet Protocol	TE	- Traffic Engineering
IPv4	- Internet Protocol version 4	ToS	- Type of Service
IPv6	- Internet Protocol version 6	VLANs	- Virtual LANs
LAN	- Local Area Network	VoIP	- Voice over Internet Protocol
MAC	- Media Access Control	VRRP	- Virtual Router Redundancy Protocol

NOTES:

1 For core and distribution components, redundancy protocol shall be the routing protocol supported. For access components, redundancy protocol shall be VRRP or equivalent protocol.

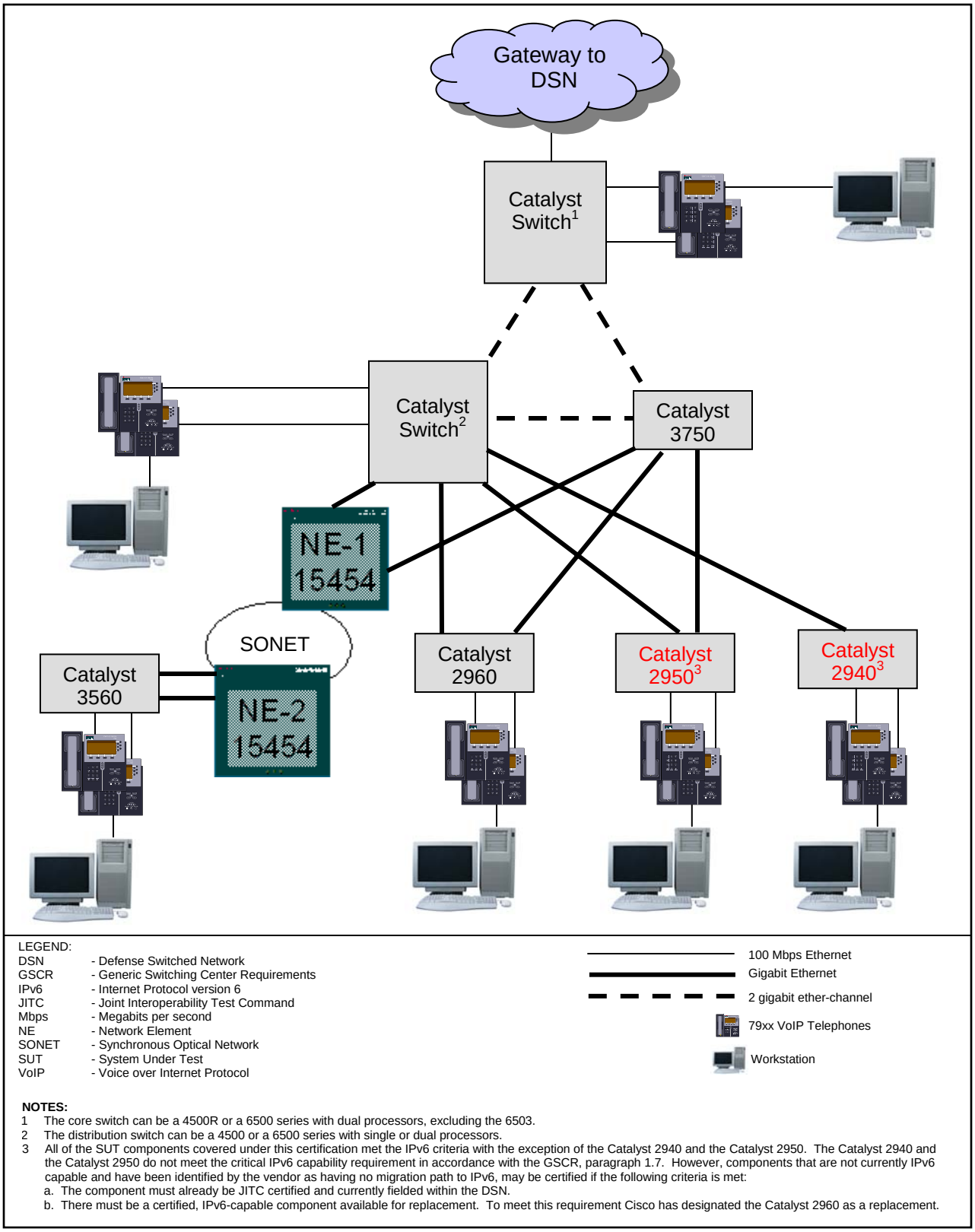
2 Verified using the Information Assurance Test Plan. Results of the security testing are published in a separate test report generated by the DISA Information Assurance test personnel.

3 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of their respective company. The vendor must state, in writing, compliance to the following criteria by 30 June 2008**:**

a. Conformant with IPv6 standards profile contained in the Department of Defense Information Technology Standards Registry (DISR).
b. Maintaining interoperability in heterogeneous environments and with IPv4.
c. Commitment to upgrade as the IPv6 standard evolves.
d. Availability of contractor/vendor IPv6 technical support.

4 Instruments connected to an access device must provide a minimum of a 10 Mbps full duplex link. For core and distribution connections, the minimum link capacity is 100 Mbps full duplex.

8. TEST NETWORK DESCRIPTION. The SUT was tested at JITC's Global Information Grid Network Test Facility in a manner and configuration similar to that of the DSN operational environment. Figures 2-3 and 2-4 depict the network topology used in testing the required functions and features of the SUT.



NOTES:

1 The core switch can be a 4500R or a 6500 series with dual processors, excluding the 6503.

2 The distribution switch can be a 4500 or a 6500 series with single or dual processors.

3 All of the SUT components covered under this certification met the IPv6 criteria with the exception of the Catalyst 2940 and the Catalyst 2950. The Catalyst 2940 and the Catalyst 2950 do not meet the critical IPv6 capability requirement in accordance with the GSCR, paragraph 1.7. However, components that are not currently IPv6 capable and have been identified by the vendor as having no migration path to IPv6, may be certified if the following criteria is met:

a. The component must already be JITC certified and currently fielded within the DSN.

b. There must be a certified, IPv6-capable component available for replacement. To meet this requirement Cisco has designated the Catalyst 2960 as a replacement.

Figure 2-3. SUT Assured Services Voice Application Local Area Network with Single Core Switch

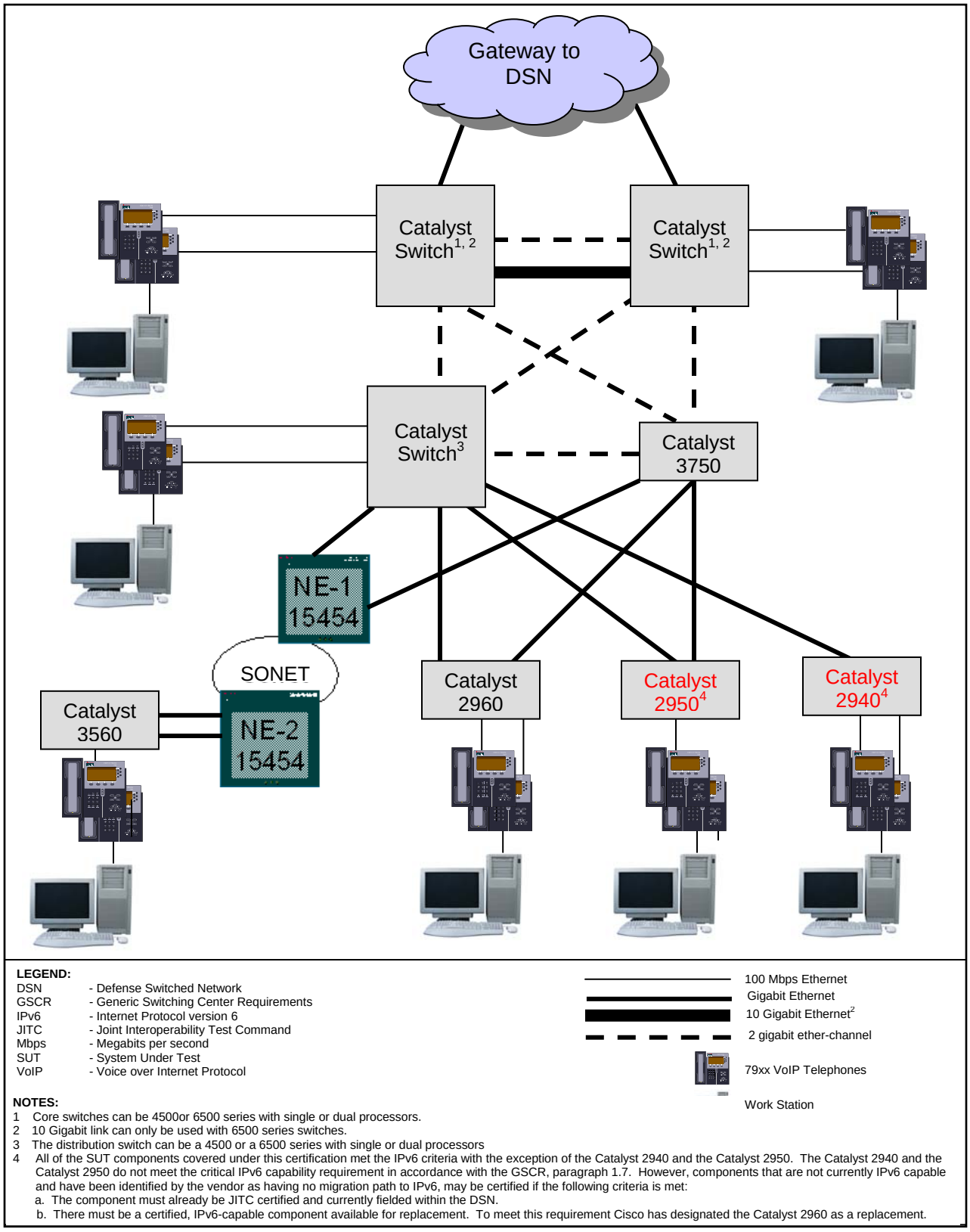


Figure 2-4. SUT Assured Services Voice Application Local Area Network with Dual Core Switches

9. SYSTEM CONFIGURATIONS. Table 2-3 provides the tested system configurations.

Table 2-3. Tested System Configurations

System Name		Software Release	
Cisco CallManager (PBX 1)		4.1(2) Service Release 1 with IOS Software Release 12.4(4)T	
System Under Test Components			
Component[1]	**Release**	**Sub-component**[1]	**Function**
Cisco **6509**/6509-NEB/ 6509-NEB-A/6503/6506/6513 Catalyst Switches	Native IOS 12.2 (18) SXF3 Release Software (fc1)	**WS-SUP720-3BXL**	Core Processor
		WS-SUP720-3B	Core Processor
		WS-SUP720	Core Processor
		WS-X6816-GBIC	16-port 1000 Mbps (Gig) fiber Interface
		WS-X6748-SFP	48-port 1000 Mbps (Gig) fiber Interface
		WS-X6724-SFP	24-port 1000 Mbps (Gig) Interface
		WS-X6704-10GE	4-port 10000 Mbps (10 Gig) Interface
		WS-X6548-GE-45AF	48-port Access switch 10/100/1000 Mbps with IEEE 802.3af PoE
		WS-X6548V-GE-TX	48-port Access switch 10/100/1000 Mbps
		WS-X6148-RJ45V	48-port Access switch 10/100/1000 Mbps
		WS-X6148-45AF	48-port Access switch 10/100/1000 Mbps
		WS-X6148A-GE-45AF	48-port Access switch 10/100/1000 Mbps
		WS-X6548-GE-TX	48-port Access switch 10/100/1000 Mbps
		WS-X6548-RJ-21	48-port Access switch 10/100 Mbps, RJ-21
		WS-X6548-RJ-45	48-port Access switch 10/100 Mbps, RJ-45
		WS-X6516-GBIC	16-port 1000 Mbps (Gig) fiber Interface
		WS-X6516A-GBIC	16-port 1000 Mbps (Gig) fiber Interface
		WS-X6516-GE-TX	16-port 10/100/1000 Mbps Interface
		WS-X6748-GE-TX	48-port Access switch 10/100/1000 Mbps
		WS-X6148V-GE-TX	48-port Access switch 10/100/1000 Mbps
		WS-X6148-RJ-45	48-port Access switch 10/100 Mbps, RJ-45
		WS-X6148-RJ-21	48-port Access switch 10/100 Mbps, RJ-21
		WS-X6148-RJ21V	48-port Access switch 10/100 Mbps, RJ-21
		WS-X6148-21AF	48-port Access switch 10/100 Mbps, RJ-21 with IEEE 802.3af PoE
		WS-X6148-GE-TX	48-port Access switch 10/100/1000 Mbps
		WS-X6148-GE-45AF	48-port Access switch 10/100/1000 Mbps with IEEE 802.3af PoE
		WS-X6148A-GE-TX	48-port Access switch 10/100/1000 Mbps
		WS-X6148A-45AF	48-port Access switch 10/100 Mbps, RJ-45 with IEEE 802.3af PoE

Table 2-3. Tested System Configurations (continued)

System Under Test Components			
Component	**Release**	**Sub-component**	**Function**
Cisco **4507R**/4503[2]/4506[2]/4510R Catalyst Switches	IOS 12.2 (31) SG	**WS-X4515 Supervisor Engine IV**	Core Processor
		WS-X4516-10GE Supervisor Engine V	Distribution Processor
		WS-X4516 (Sup V)	Distribution Processor
		WS-X4306-GB	6-port 1000 Mbps (Gig) Interface
		WS-X4302-GB	2-port 1000 Mbps (Gig) Interface
		WS-X4148-RJ45V	48-port Access switch 10/100 Mbps, RJ-45
		WS-X4148-RJ45	48-port Access switch 10/100 Mbps, RJ-45
		WS-X4124-RJ45	24-port Access switch 10/100 Mbps, RJ-45
		WS-X4148-RJ21	48-port Access switch 10/100 Mbps, RJ-21
Catalyst 3750[2] – (WS-C3750G-12S-E)	12.2 (25) SEE		Distribution switch 12-port 1000 Mbps (Gig) fiber Interfaces
Catalyst 3560 – with IEEE 802.3af PoE / Catalyst 3560	12.2 (25) SEE2		24-port Access switch 10/100 Mbps
Catalyst 2960	12.1 (25) SEE		48-port Access switch 10/100 Mbps
Catalyst 2950 [3]	12.2 (22) EA7		48-port Access switch 10/100 Mbps
Catalyst 2940 [3]	12.1 (22) EA7		8-port Access switch 10/100 Mbps
ONS 15454	Release 7.0	**15454-ML1000-2-NSE**	1000 Mbps Ethernet, 2 SFP slots, Layer 2/3 switching, SONET/ANSI system
		15454-ML100T-12	12 port 10/100 Ethernet card
		15454-TCC2P	Timing, Communications and Control Card, Version 2 Plus
		15454-XC-VXC-10G	60 Gig/5 Gig high-order/low-order cross-connect card, XC-VXC-series, I-Temp, SONET system
		15454-XC-10G-S1	OC-192 short range card
		15454-MRC-12	Dual-rate OC-12/STM-4 and OC-3/STM-1 1310 nm SMF, SFP module

LEGEND:

802.3af	- Standard for Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI)
AF	- PoE IEEE 802.3af Standard
ANSI	- American National Standards Institute
B/BXL	- Version B, eXtra Large Memory
DoD	- Department of Defense
DSN	- Defense Switched Network
G, GB, Gig	- Gigabit
GBIC	- Gigabit Interface Card
GE	- Gigabit Ethernet
E	- Ethernet
IEEE	- Institute of Electrical and Electronics Engineers, Inc.
IOS	- Internetworking Operating System
IPv6	- Internet Protocol version 6
JITC	- Joint Interoperability Test Command
Mbps	- Megabits per second
ML	- Multilayer
MRC	- Multirate Optic Card
NEB	- Network Equipment Building
nm	- nanometer
NSE	- Network Services Engine
OC	- Optical Carrier
ONS	- Optical Network System
PBX 1	- Private Branch Exchange 1
PoE	- Power Over Ethernet
RJ	- Registered Jack
SFP	- Small Form Factor Pluggable
SMF	- Single Mode Fiber
SONET	- Synchronous Optical Network
STM	- Synchronous Transport Module
SUP	- Supervisor
TCC2P	- Timing, Communications and Control - version 2 Plus
TX	- Twisted Pair
V	- Voice
VXC	- Very Large Cross Connect
WS	- Workgroup Station
XC	- Cross Connect

NOTES:

1 Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same IOS software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.

2 Indicates these switches support one processor and must be configured to fail over to a second distribution switch.

3 All of the SUT components covered under this certification met the IPv6 criteria with the exception of the Catalyst 2940 and the Catalyst 2950. The Catalyst 2940 and the Catalyst 2950 do not meet the critical IPv6 capability requirement in accordance with the GSCR, paragraph 1.7. However, components that are not currently IPv6 capable and have been identified by the vendor as having no migration path to IPv6, may be certified if the following criteria are met:

a. The component must already be JITC certified and currently fielded within the DSN.

b. There must be a certified, IPv6-capable component available for replacement. To meet this requirement Cisco has designated the Catalyst 2960 as a replacement.

10. TESTING LIMITATIONS. None.

11. TEST RESULTS

a. Components. The SUT met the minimum interoperability requirements of the GSCR, appendix 3, for an ASVALAN. The network consisted of three main components: core switches, distribution switches, and access switches. The results for the specific tests carried out are provided below.

(1) Class of Service (CoS). The GSCR, appendix 3, section A3.3.2, outlines several methodologies to implement CoS. The SUT employed IEEE 802.1p at the Data Link Layer (L2) and Differentiated Services Code Point (DSCP) at the Network Layer (L3) and 802.1p to DSCP mapping, which was verified by capturing packets at both layers within the network.

(2) Traffic Prioritization. Priorities were applied in accordance with the CoS listed above. This ensured voice signaling would get the highest level of priority; voice media stream would be prioritized lower than voice signaling but higher than data, and data traffic would receive the lowest priority. At L2, packets were tagged as: Data traffic = 0, Voice media = 5, and Voice Signaling and Network Management = 3. Trust DSCP and trust CoS statements were applied between all ports. By filling uplinks to their capacity with data packets tagged at 0, we were able in inject voice packets, tagged with 5 and 3 and ensure they received precedence and were not delayed.

In addition, flooding parameters were set to prevent broadcast and multicast traffic from overwhelming the ports. Broadcast limits were set to 5% and multicast limits were set to 70%. The configuration changes that were made to ensure proper operation can be found on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.

(3) QoS. Packets tagged with a CoS of 3 are queued in the high priority queue. The CoS values 5 and 0 are serviced in separate Weighted Round Robin or Shaped Round Robin queues, with 5 receiving a higher weight value therefore, it will be serviced more frequently then 0. These tags were used to identify and separate traffic types as it passed through network connections ensuring voice traffic takes precedence over data traffic. For L3 DSCP, packets tagged 0, 5, and 3 were marked 0, 46, and 48 respectively. Again, by filling uplinks to their capacity with data packets tagged at 0, we were able in inject voice packets, tagged with 5 and 3 and ensure they received treatment in a high queue and were not delayed throughout the network.

(4) Policing. The SUT implemented Class Based Weighted Fair Queuing that uses DSCP values to define how traffic is treated at each individual network node. DSCP values are used from the L3 IP header.

(5) Virtual LAN (VLAN). JITC tested port-based VLANs. Switches within the topology were configured with multiple VLANs using the IEEE 802.1Q tag to separate data from voice traffic. Media Access Control address and Protocol-based VLANs were verified through LoC.

(6) IEEE Conformance. All aspects of IEEE conformance were met through the LoC or testing. All test results are discussed under their respective topics.

(7) Reliability. The GSCR, appendix 3, section A3.3.4.1, requires that there be no single point of failure within the network that can cause an outage of more than 64 telephony subscribers. In order to meet the availability requirement, all switching/routing platforms that offer more than 64 telephony subscribers shall have a modular chassis that provides at a minimum dual power supplies, dual processors, redundancy protocol, and switch fabric redundancy. To meet this requirement, all links connected between the cores, core and distribution, and between the distribution switches, as shown in figure 2-3 and 2-4 are configured as Port-Channels. Two-Gigabit Port-Channels must be configured on all these links. A Gigabit Port-Channel is an aggregation of two one-gigabit fiber ports to form a single two-gigabit fiber port-channel. The two fiber links must be terminated onto separate fiber cards at each switch.

The processors on the 6500 series and 4507R switches must be configured for "Stateful Switch Over (SSO)", which is configured under the redundancy command. "Non-stop forwarding" (NSF) must be set within the router under Open Shortest Path First (OSPF) configuration. NSF with SSO is a supervisor redundancy mechanism on the Supervisor Engines. In conjunction with SSO, NSF works to ensure L3 integrity following a switchover. Non-stop forwarding allows a router experiencing the failure of an active supervisor to continue forwarding data packets along known routes while the routing protocol information is recovered and validated. NSF relies on the separation of the control plane and the data plane during supervisor switchover. The data plane continues to forward packets based on pre-switchover Cisco Express Forwarding information. The control plane implements graceful restart routing protocol extensions to signal a supervisor restart to NSF-aware neighbor routers, inform its neighbor adjacencies, and rebuild its routing protocol database following a switchover.

(8) Network Management. The GSCR, appendix 3, section A3.3.4.2, requires that the vendor provide a management system to monitor the performance of the LAN portion of the VoIP system. Due to numerous third party systems and applications capable of performing this function, this requirement was verified via LoC.

(9) Security. Security requirements in accordance with the GSCR, appendix 3, section A3.3.4.3, were verified using the Information Assurance Test Plan. Results of the security testing are reported in a separate test report generated by the DISA Information Assurance test personnel.

(10) Internet Protocol version 6 (IPv6). An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of Internet Protocol version 4 (IPv4). IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of their

respective company. The vendor stated, in writing, compliance to the following criteria by 30 June 2008:

(a) Conformant with IPv6 standards profile contained in the DoD Information Technology Standards Registry (DISR).

(b) Maintaining interoperability in heterogeneous environments and with IPv4.

(c) Commitment to upgrade as the IPv6 standard evolves.

(d) Availability of contractor/vendor IPv6 technical support.

OSPF version two was used during the tests. OSPF version three will be required for IPv6 compatibility. All of the SUT components covered under this certification met the IPv6 criteria with the exception of the Catalyst 2940 and the Catalyst 2950. The Catalyst 2940 and the Catalyst 2950 do not meet the critical IPv6 capability requirement in accordance with the GSCR, paragraph 1.7. However, components that are not currently IPv6 capable and have been identified by the vendor as having no migration path to IPv6, may be certified if the following criteria are met:

a. The component must already be JITC certified and currently fielded within the DSN.

b. There must be a certified, IPv6-capable component available for replacement. To meet this requirement Cisco has designated the Catalyst 2960 as a replacement.

(11) Traffic Engineering

(a) Links. Two Gigabit Port-Channels were configured between the core switches, between the core and distribution switches, and between the distribution switches. These were configured to separate fiber cards on each switch to ensure proper redundancy. Gigabit Port-Channel is a high-performance Ethernet technology that provides gigabit per second transmission rates. Port-Channels provide flexible, scalable bandwidth with resiliency and load sharing across links for switches and router interfaces. In addition to the two gigabit Port-Channels between the 6500 core elements, a 10-gigabit fiber was utilized. The high-speed link added additional bandwidth, however redundant fiber links must exist as shown in figure 2-4.

Trunk Protocol Negotiation was changed from its default “Desirable” to “Mode on.” Configuring the trunk mode as “on” on both sides of the link will allow the trunk to come up without a Dynamic Trunking Protocol negotiation agreement.

(b) Scalability. The SUT can be scaled to meet any number of IP phone subscribers as long as the SUT is composed of the equipment and software listed in table 2-3, and are consistent with traffic engineering constraints contained in the GSCR,

appendix 3. Table 2-4, which was approved by the DSN Configuration Control Board (DSN CCB) on Dec 2004, outlines the maximum number of subscribers that can be supported per each link capacity.

Table 2-4. IP Subscriber Supportability by Link Capacity

Link Type	LAN BW	Users
Non-Converged	10 Mbps	64[1]
	100 Mbps	64[1]
	1 Gbps	64[1]
	10 Gbps	64[1]
	10 Mbps LP	100[2]
	100 Mbps LP	1000[2]
	1 Gbps LP	10000[2]
	10 Gbps LP	100000[2]
Converged	10 Mbps	25[3]
	100 Mbps	64[1]
	1 Gbps	64[1]
	10 Gbps	64[1]
	10 Mbps LP	25[3]
	100 Mbps LP	250[4]
	1 Gbps LP	2500[4]
	10 Gbps LP	25000[4]

LEGEND:

BW	- Bandwidth	LAN	- Local Area Network
Gbps	- Gigabits per second	LP	- Link Pair
IP	- Internet Protocol	Mbps	- Megabits per second
kbps	- kilobits per second		

NOTES:

1 For single links, number of users is limited to a maximum of 64 because of single point of failure requirements.
2 The number of users is calculated as bandwidth (BW) divided by 100 kbps per user.
3 The number of users was limited to 64 users per note 1 or 25% of total users per note 1, whichever was less.
4 For the converged network, voice traffic was engineered not to exceed 25 % of total utilization using an estimated 100 kbps per voice call.

(12) LAN Architectures. OSPF was implemented between the 6500 and the 4507R core routers, the 4507R and 3750 distribution layer, and the 3560 at the access layer to meet failover requirements. OSPF utilizes link-state protocols to identify lowest cost paths within the LAN. Additionally, OSPF is an open standard, and would likely be a common protocol between different vendors equipment. Cisco's implementation of OSPF allows for sub-second Hello packets for rapid failed path detection. All links were configured for the default of 10 second Hello Packets except for the link to the ONS. The Hello Packets routed via the ONS were configured for a 200ms hello packet, which brought failure time from 30 seconds to under the 2 second requirement. Additionally, Hot Standby Router Protocol (HSRP) was utilized in the same areas as OSPF with the exception of the 3560 access. HSRP supports rapid failover for L2 access switches within the architecture. Measured failover for the L2 switches and paths was also less than two seconds. These rapid responses were due to HSRP running between key elements of the SUT.

(a) Delay. According to the GSCR, appendix 3, section A3.3.1.1, the one-way packet delay, shall be five milliseconds (ms) or less, as measured over a five-minute period. The average one-way delay for each of 50 five-minute periods, measured between the access and core devices, was 0.13 ms, with a maximum delay of 0.80 ms.

(b) Jitter. The SUT utilizes a dynamic jitter buffer in the IP phones, which cannot be adjusted. The egress jitter buffer in all gateways was set for a fixed duration of 20 ms. With a 100% bandwidth load, jitter was measured to be 0 ms over a five-minute period. This met the 5 ms requirement established by section A3.3.1.2, appendix 3 of the GSCR.

(c) Packet Loss. Network packet loss occurs when packets are sent, but not received at the final destination. The GSCR, appendix 3, section A3.3.1.3, states that LANs shall be engineered so the measured voice packet loss within the LAN shall not exceed 0.05% averaged over any five-minute period. With 100% bandwidth load, the measured packet loss was 0.00% over a 24-hour period.

(13) Network Element. The Cisco ONS 15454 was used to carry VoIP and data traffic during the test. The ML-1000-2 1-Gigabit fiber optic card was used to interface IP traffic. Traffic generated only represented ten percent of the carrying capacity of the SONET loop. The IP load did not represent a significant load to the system; therefore, prioritization of information over the ONS was not evaluated. The evaluation demonstrated the ML-1000-2 operated as expected and did not exhibit more than 0.05% packet loss. The L2 and L3 traffic exited the ONS properly tagged. Failover between links performed within two seconds when the OSPF Hello Packet interval was reduced from the default of 10 seconds to one-twentieth of a second. Other cards and elements within the ONS were not evaluated in this test; however, other components were tested and covered under a separate report.

b. System Interoperability Results. The SUT including VoIP is certified for joint use within the DSN as an ASVALAN in accordance with the requirements set forth in the GSCR, appendix 3. The system interoperability test summary is shown in table 2-5 and the detailed component interoperability test status is shown table 2-6.

12. TEST AND ANALYSIS REPORT. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil (NIPRNet), or http://199.208.204.125 (SIPRNet). Information related to DSN testing is on the TSSI website at http://jitc.fhu.disa.mil/tssi.

Table 2-5. SUT System Interoperability Test Summary

Device Requirement	Reference	Test Results	Remarks
Delay measured at 5 ms or less	GSCR, Appendix 3, A3.3.1.1	Met	
Jitter measured at less than 5 ms	GSCR, Appendix 3, A3.3.1.2	Met	
Packet Loss less than 0.05%	GSCR, Appendix 3, A3.3.1.3	Met	
Reliability	GSCR, Appendix 3, Section A.3.3.4.1	Met	
IPv6	GSCR, Appendix 3, Section A3.2.8	See note 1.	
Security	GSCR, Appendix 3, A3.2.4	See note 2.	

LEGEND:

DISA	- Defense Information Systems Agency	IPv4	- Internet Protocol version 4
DISR	- DoD Information Technology Standards Registry	IPv6	- Internet Protocol version 6
DoD	- Department of Defense	ms	- millisecond
GSCR	- Generic Switching Center Requirements	SUT	- System Under Test

NOTES:

1 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of their respective company. The vendor stated, in writing, compliance to the following criteria by 30 June 2008:
   a. Conformant with IPv6 standards profile contained in the DISR.
   b. Maintaining interoperability in heterogeneous environments and with IPv4.
   c. Commitment to upgrade as the IPv6 standard evolves.
   d. Availability of contractor/vendor IPv6 technical support.

2 Security is tested by DISA-led Information Assurance test teams and published in a separate report.

Table 2-6. Component Interoperability Test Summary

DSN Line Interfaces						
Interface	**Component[1]**	**Status**	**Device Requirement**	**Test Results**	**Reference**	**Remarks**
1000BaseFX 100/1000 BaseTX	Cisco **6509**/6509-NEB/ 6509-NEB-A/6503/6506/ 6513 Catalyst Switches	Certified as: Core Distribution Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	
			Security	See note 3.	GSCR, Appendix 3, A.3.3.4.3	
			IPv6	See note 4.	GSCR, Appendix 3, A3.2.8, Paragraph 1.7	
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	
1000BaseFX 100/1000 BaseTX	Cisco **4507R**/4503[2]/4506[2] /4510R Catalyst Switches	Certified as: Core Distribution Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	
			Security	See note 3.	GSCR, Appendix 3, A.3.3.4.3	
			IPv6	See note 4.	GSCR, Appendix 3, A3.2.8, Paragraph 1.7	
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	
1000BaseFX	**Catalyst 3750**	Certified as: Distribution	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	
			Security	See note 3.	GSCR, Appendix 3, A.3.3.4.3	
			IPv6	See note 4.	GSCR, Appendix 3, A3.2.8, Paragraph 1.7	
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	

Table 2-6. Component Interoperability Test Summary (continued)

DSN Line Interfaces						
Interface	**Component**	**Status**	**Device Requirement**	**Test Results**	**Reference**	**Remarks**
1000BaseFX 100BaseTX	**Catalyst 3560** – PoE 24 **Catalyst 2950**[5] – Inline Power **Catalyst 2960** – Inline Power **Catalyst 2940**[5] – Inline Power	Certified as: Access	TE	Met	GSCR, Appendix 3, A.3.3.4.4	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	
			Security	See note 3.	GSCR, Appendix 3, A.3.3.4.3	
			IPv6	See note 4.	GSCR, Appendix 3, A3.2.8, Paragraph 1.7	See note 5.
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	

Table 2-6. Component Interoperability Test Summary (continued)

DSN Line Interfaces						
Interface	**Component**	**Status**	**Device Requirement**	**Test Results**	**Reference**	**Remarks**
1000BaseFX	**ONS 15454**	Certified as: Network Element Transport	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	
			Security	See note 3.	GSCR, Appendix 3, A.3.3.4.3	
			IPv6	See note 4.	GSCR, Appendix 3, A3.2.8, Paragraph 1.7	
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	

LEGEND:

100/1000BaseTX	- 100/1000 Mbps Ethernet over Category 5 Twisted Pair Copper
1000BaseFX	- 1000 Mbps Ethernet over fiber
CoS	- Class of Service
DISA	- Defense Information Systems Agency
DISR	- DoD Information Technology Standards Registry
DoD	- Department of Defense
DSN	- Defense Switched Network
GSCR	- Generic Switching Center Requirements
IEEE	- Institute of Electrical and Electronics Engineers, Inc.
IOS	- Internetworking Operating System
IPv4	- Internet Protocol version 4
IPv6	- Internet Protocol version 6
JITC	- Joint Interoperability Test Command
LoC	- Letters of Compliance
Mbps	- Megabits per second
NEB	- Network Equipment Building
ONS	- Optical Network System
PoE	- Power Over Ethernet
QoS	- Quality of Service
TE	- Traffic Engineering
VLAN	- Virtual Local Area Network

NOTES:

1 Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same IOS software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.

2 Indicates these switches support one processor and must be configured to fail over to a second distribution switch.

3 Security is tested by DISA-led Information Assurance test teams and published in a separate report.

4 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of their respective company. The vendor stated, in writing, compliance to the following criteria by 30 June 2008:
   a. Conformant with IPv6 standards profile contained in the DISR.
   b. Maintaining interoperability in heterogeneous environments and with IPv4.
   c. Commitment to upgrade as the IPv6 standard evolves.
   d. Availability of contractor/vendor IPv6 technical support.

5 All of the SUT components covered under this certification met the IPv6 criteria with the exception of the Catalyst 2940 and the Catalyst 2950. The Catalyst 2940 and the Catalyst 2950 do not meet the critical IPv6 capability requirement in accordance with the GSCR, paragraph 1.7. However, components that are not currently IPv6 capable and have been identified by the vendor as having no migration path to IPv6, may be certified if the following criteria are met:
   a. The component must already be JITC certified and currently fielded within the DSN.
   b. There must be a certified, IPv6-capable component available for replacement. To meet this requirement Cisco has designated the Catalyst 2960 as a replacement.